Novembre 2019
Numéro 4

LA GAZETTE DU GDR

Sécurité Informatique - GDR2046

Édito du directeur

La rentrée du GDR a été marquée par l'organisation de la quatrième édition des Rencontres Entreprises DOCtorants en Sécurité (REDOCS), qui ont eu lieu comme chaque année sur le campus CNRS de Gif-sur-Yvette pendant les vacances de la Toussaint. Pilotées par Pascal Lafourcade (LIMOS), les REDOCS ont accueilli cette année EDF, Thales et SystemX, ainsi que quinze doctorants. Certaines candidatures de doctorants n'ont pu être retenues en raison de la forte demande. Rendez-vous en octobre 2020 pour la cinquième édition !

Les Groupes de Travail (GT) sont également très actifs en cette rentrée, avec une journée (27 novembre) du GT *Sécurité des systèmes, des logiciels et des réseaux* (SSLR) sur les « outils pour construire, valider, corriger et auditer la sécurité du code en prenant en compte l'évolution des attaques », organisée par O. Levillain, A. Francillon et V. Guyot à l'ESIEA (Paris) ; une journée (29 novembre) du GT *Sécurité et données multimédia* (SDM) – qui est commun avec le GDR ISIS – sur les « tendances en évaluation de la qualité pour la compression et la sécurisation des contenus émergents », organisée par A. Chetouani, G. Valenzise et C. Larabi à la délégation CNRS Paris-Villejuif (Site d'Ivry-sur-Seine).

Nous connaissons d'autre part certaines dates pour 2020 : K. Heydemann et D. Couroussé organiseront la journée annuelle du GT *Méthodes formelles pour la sécurité* (MFS) le 30 janvier 2020 au LIP6 (Paris). G. Blanc et O. Levillain organiseront RESSI du 18 au 20 mai 2020, à Nouan-le-Fuzelier, en Sologne, dans le cadre du GT *Sécurité des systèmes, des logiciels et des réseaux* (SSLR). A. Roux-Langlois, M. Sabt, O. Sanders et D. Vergnaud organiseront les journées C2 du 15 au 20 mars à Erdeven en Bretagne. Notez également la date de l'école d'été, qui aura lieu au château du CNRS de Gif-sur-Yvette du 6 au 10 juillet 2020, organisée par S. Bardin et S. Delaune.

Je profite de cette opportunité pour remercier toutes les personnes qui s'impliquent dans la vie du GDR, notamment à travers l'organisation d'événements.

Après ces diverses annonces, je vous souhaite une bonne lecture, avec notamment une présentation du *Grenoble Alpes Cybersecurity Institute* par Marie-Laure Potet et Romain Xu-Darme dans la rubrique *En direct des labos*, un *Retour sur l'école d'été* par Matthieu Mastio, ainsi qu'une interview de Pierrick Gaudry dans le petit *coin prospectif*.

Gildas Avoine

Rubriques

Événements

(Repris en partie du forum du GDR)

Workshop BotConf *Bordeaux, France, 4-6 décembre 2019*

International Conference on Information Security Theory and Practice *Paris, 11–12 décembre 2019*

Conférence Principles of Secure Compilation (PriSC) *New Orleans, États-Unis, 25 janvier 2020*

Conférence Innovation in Clouds, Internet and Networks *Paris, France, 24-27 février 2020*

Conférence Computer Security track (SEC@SAC20) *Brno, République tchèque, 30 mars - 3 avril 2020*

Journées Journées Codage & Cryptographie *Erdeven, France, 15-20 mars 2020*

Symposium sur la sécurité des technologies de l'information et des communications *Rennes, France, 3 - 5 juin 2020*

Conférence Computer Security Foundations Symposium *Boston, États-Unis, 22-25 juin 2020*

En direct des labos

Marie-Laure Potet , Romain Xu-Darme

Pour ce numéro, la gazette a choisi d'interviewer non pas un laboratoire mais le consortium de laboratoires grenoblois en cybersécurité. Nous sommes donc allés rencontrer Marie-Laure Potet et Romain Xu-Darme, tous les deux membres de cet institut, pour qu'ils nous le présentent.

Bonjour Marie-Laure, bonjour Romain, quelles entités participent au « Grenoble Alpes Cybersecurity Institute » ?

Le Grenoble Alpes Cybersecurity Institute, que nous appelons plus simplement le Cyber@Alps, fédère les chercheurs de 16 laboratoires du périmètre de l'Idex Univ. Grenoble Alpes (Institut Fourier, CESICE, CEA-LETI, Inria, Verimag, LCIS, LIG, TIMA, LJK, CREG, LISTIC, CERAG, G2Elab, G-SCOP, Gipsa-lab, Pacte) travaillant sur les domaines de la cybersécurité et de la protection de la vie privée. Cela représente une communauté d'environ 100 permanents et 50 non-permanents répartis dans deux communautés, d'une part la communauté Mathématiques, Sciences et Technologies de l'Information et de la Communication (dont une forte implication de l'institut LETI du CEA), d'autre part la communauté Sciences Sociales.

Quels sont les objectifs de cet institut ?

La construction du projet Cyber@Alpsvise trois objectifs. Le premier est de continuer à structurer la communauté en favorisant notamment l'interdisciplinarité, d'abord entre chercheurs de domaines « proches » comme les mathématiques, l'informatique et la microélectronique, mais également en bâtissant des ponts avec des chercheurs venant de domaines plus éloignés comme le droit international et les sciences économiques ou politiques. Cette structuration a démarré il y a maintenant 8 ans dans le cadre d'une équipe transverse du Labex Persyval, puis le réseau AMNECYS, rejoignant nos collègues juristes ayant déjà leurs propres activités dans ce domaine.

Le second objectif est d'avancer ensemble sur des grands défis du domaine d'une part en prenant en compte l'impact sociétal de la cybersécurité dans les solutions techniques et, réciproquement, en intégrant les aspects technologiques dans les défis sociétaux. Par exemple, nous nous intéressons aux processus de réglementation ou de certification en prenant en compte conjointement leur mise en œuvre technique, les assurances que l'on peut en tirer et leur acceptation sociétale. Cette approche holistique nous permet d'intégrer la recherche fondamentale dans un contexte plus large et donc, nous l'espérons, plus pertinent.

Enfin, le dernier objectif est d'augmenter la visibilité de la communauté locale, qui a ses propres particularités au niveau national, par exemple dans le champ de la sécurité matérielle. Un grand nombre d'équipements de recherche qui préexistaient à la création de l'institut sont disponibles. On peut citer en exemple les plateformes de simulation de systèmes industriels permettant de rejouer des scénarios de cyberattaques, d'intégrer nos mécanismes de protections et d'en tester la robustesse. Cet écosystème est également enrichi par la présence à proximité de leaders industriels, d'infrastructures de recherche à l'état de l'art mondial comme les salles blanches du CEA-Leti ou encore un des trois CESTI Hardware du schéma français de certification, qui permet de valider la sécurité de nouvelles technologies sur des équipements d'attaques au-delà de l'état de l'art.

« Cette approche holistique nous permet d'intégrer la recherche fondamentale dans un contexte plus large... »

La présence sur le territoire de l'Institut de Recherche Technologique (IRT) Nanoelec, avec qui nous avons une collaboration étroite, permet la réalisation et l'évaluation de démonstrateurs, en lien avec les partenaires industriels de Nanoelec, afin d'accélérer le transfert et la valorisation de certaines briques technologiques développées dans Cyber@Alps.

Une composante forte de cet institut est donc l'interdisciplinarité. Pouvez-vous nous donner des exemples de recherches interdisciplinaires ?

Nous distinguons deux types d'interdisciplinarité : l'interdisciplinarité interne qui fait collaborer les chercheurs du sillicium aux solutions sécurisées prouvées et l'interdisciplinarité « externe » qui lie sciences du numérique et sciences sociales. Même dans le premier cas, ceci n'est pas si simple et demande à chacun d'appréhender et de comprendre les problématiques de collègues appartenant à d'autres domaines de recherche. Pour cela nous organisons des ateliers thématiques abordant les différentes facettes, comme le workshop organisé dans le cadre du mois européen de la cybersécurité autour de la protection des données qui a réuni des informaticiens, des juristes et les RSSI et DPO de la métropole Grenoble Alpes.

En termes de soutien à la recherche, nous finançons ou cofinançons sept thèses toutes co-encadrées par deux laboratoires. Citons par exemple une thèse codirigée par l'équipe Privatics de Inria et le CESICE sur la problématique de la régulation des cyberarmes et l'attribution des cyberattaques et une thèse codirigée par le Laboratoire Jean-Kuntzmann et le CERAG sur l'impact des technologies de la blockchain sur les marchés financiers, deux sujets de recherche nécessitant des connaissances à la fois techniques et juridiques ou économiques.

Cybersecurity Institute
Univ. Grenoble Alpes
Reshaping technologies and social sciences

L'interdisciplinarité interne s'est déjà fortement concrétisée dans le Cyber@Alps en regroupant des personnes travaillant sur des thèmes complémentaires. Par exemple, nous avons été nombreux à participer au projet PIA Aramis, porté par ATOS WG, en couvrant des aspects transverses de la sécurité allant d'une architecture de sécurité permettant l'isolation des flux, incluant la conception d'un crypto-module, la vérification de protocoles industriels type Modbus et OPC-UA, et la proposition de solutions pour la gestion du cycle de vie.

« Nous finançons ou co-finançons sept thèses toutes co-encadrées par deux laboratoires. »

De nouvelles collaborations se mettent en place, par exemple dans le domaine des attaques en faute nous collaborons le CEA, le LCIS, TIMA et Vérimag afin de couvrir le processus global de mise en œuvre des attaques, de leur effet sur les codes embarqués et de l'outillage permettant d'évaluer et de rendre robustes ces applications. Un autre thème fédérateur est la réalisation de crypto-modules à l'état de l'art. Enfin, nous pouvons aussi citer le projet EASIMOB, piloté par deux partenaires industriels, et qui a été récemment sélectionné par l'ANR lors de l'appel à projet Flash JOP2024 pour la sécurisation de sites sensibles lors des Jeux Olympiques et Paralympiques de Paris 2024. Ce projet, porté par l'Institut Fourier, impliquera des chercheurs de différents laboratoires du Cyber@Alps.

Quels sont les autres challenges scientifiques qui vous intéressent au sein de l'institut ?

Nous appliquons notre démarche interdisciplinaire sur différents axes de recherche comme les éléments sécurisés à bas coût destinés au marché de l'IoT, les infrastructures critiques sécurisées et leur gestion en termes de cycle de vie, mais également l'analyse de vulnérabilités matérielles et logicielles. Nous tentons par ailleurs d'apporter des réponses à des défis globaux comme la régulation du cyberespace, la protection de la vie privée ou l'augmentation de la résilience pratique dans l'industrie et la société.

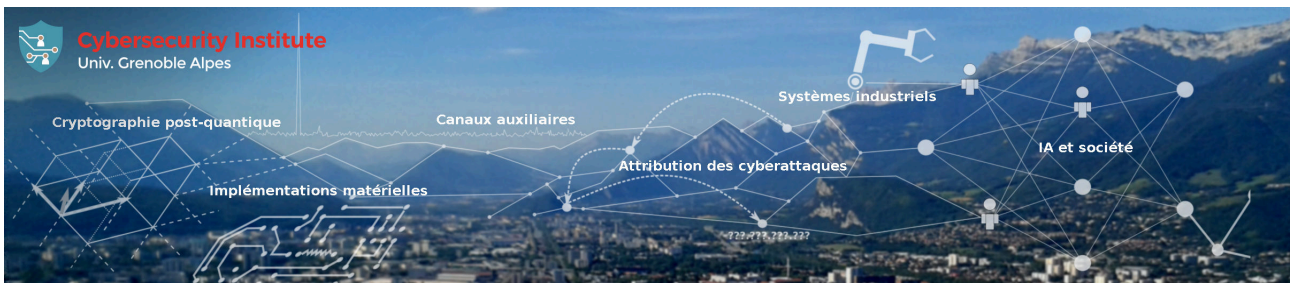
Pour finir, pouvez-vous nous rappeler quelles sont les formations qui sont adossées à cet institut ?

L'Université Grenoble Alpes propose plusieurs formations de niveau M2 en cybersécurité dont les principales sont un parcours Cybersécurité orienté vers l'international (cours en anglais), un parcours Cybersécurité et Informatique Légale en alternance ; un parcours Sécurité Internationale et Défense et un parcours Carrières juridiques internationales (Faculté de droit). Nous promouvons les valeurs de l'interdisciplinarité auprès de nos étudiants de filières techniques et juridiques en organisant un challenge mixte mélangeant gestion de crise et recherche de preuves numériques. Une équipe mixte d'étudiants des Masters « Cybersécurité & Informatique Légale », « Sécurité Internationale & Défense » et « Carrières juridiques internationales » a d'ailleurs atteint les demi-finales du Strategy Challenge du FIC 2019. Une liste plus complète des formations en lien avec le Cybersecurity Institute est disponible sur notre site `cybersecurity.univ-grenoble-alpes.fr`.


Marie-Laure Potet et Romain Xu-Darme.

Merci Marie-Laure, merci Romain et bonne continuation à Grenoble !

Article rédigé par Marie-Laure Potet (Grenoble-INP, Verimag), Romain Xu-Darme (UGA) et Patrick Bas. Projet porté par Philippe Elbaz-Vincent (UGA/Institut Fourier), Claude Castelluccia (Inria Privatics), Karine Bannelier (UGA/CESICE), Bruno Charrat (CEA-LETI) et Marie-Laure Potet (Grenoble INP/VERIMAG),
Contact : Marie-Laure.Potet@univ-grenoble-alpes.fr, romain.xu@univ-grenoble-alpes.fr



Retour sur l'école d'été

Matthieu Mastio, participant

Le GDR sécurité informatique a profité des beaux jours rennais pour y organiser, du 8 au 12 juillet, l'école d'été SILM. Cet événement a réuni de nombreux spécialistes de la sécurité informatique, issus aussi bien du monde académique qu'industriel, dans les locaux d'INRIA et de CentraleSupélec.

Les écoles d'été sont des événements à part dans le monde de la recherche, puisqu'elles permettent d'aborder des sujets parfois très pointus, tout en prenant en compte le fait que l'auditeur n'est pas nécessairement spécialiste dans le domaine. Les présentations données sont ainsi généralement plus longues que ce que l'on a coutume de voir dans les conférences, puisque l'intervenant va généralement prendre le temps de présenter les bases de sa discipline avant d'entrer dans le vif du sujet.

Ce type d'événements est en outre l'occasion de rencontrer pendant toute une semaine des experts reconnus venant du monde entier. En plus de permettre de s'immerger dans un domaine particulier, c'est aussi l'occasion rêvée pour établir un premier contact avec un futur employeur, ou de commencer une collaboration fructueuse avec une autre équipe.

L'objectif du semestre "Sécurité Logicielle et Matérielle" (SILM) est de rapprocher les communautés expertes dans les domaines de la sécurité informatique, tant matérielle que logicielle. Clémentine Maurice, Frédéric Tronel et Lydie Mabil, les organisateurs de l'école d'été SILM nous ont gâtés, puisqu'ils ont réussi à faire venir des grands noms appartenant à ces deux disciplines.

Nous avons ainsi eu la chance d'assister à des présentations de grandes qualités, où nous avons par exemple pu apprendre que certains des mécanismes de sécurité les plus performants mis en place pour nous protéger pouvaient être mis à mal par des attaques par canaux auxiliaires relativement simples à mettre en œuvre. Après une plongée passionnante dans les méandres du *reverse engineering*, nous avons eu aussi droit à un cours détaillé d'architecture matérielle, nous rappelant à quel point la manière dont nous concevons notre ordinateur est caduque.

Un point intéressant soulevé lors de cette semaine était que toutes les méthodes déployées jusqu'à présent par Intel pour contrecarrer SPECTRE sont inefficaces, et que nos ordinateurs sont toujours à la merci d'attaquants sans scrupule. Mais, comme n'a pas manqué de le faire remarquer l'un des intervenants, les attaques par canaux auxiliaires ne sont pas réservées qu'aux machines : nous aussi pauvres humains pouvons être la cible d'attaques sophistiquées, exploitant des corrélations dans nos comportements afin de nous espionner.

Il était toutefois permis de garder espoir, puisque certaines présentations se sont concentrées sur les défenses qu'il est possible de déployer contre ces attaques pernicieuses. Rassurez vous, nos chercheurs s'emploient à collecter et trier de manière systématique un grand nombre de logiciels malveillants, à créer de nouveaux algorithmes permettant le masquage ou l'obfuscation polymorphique des canaux auxiliaires. Lors de l'école, ils nous ont proposé également des contres mesures, cette fois-ci efficaces, contre l'attaque SPECTRE et ses dérivées.

Nos écoliers et leurs professeurs.

Après toutes ces heures passées dans l'amphi, il fût temps de mettre toutes ces nouvelles connaissances en pratique. C'est pour cette raison que trois TP nous ont été proposés. Le premier nous a initié aux méthodes permettant de casser nous-mêmes les algorithmes de cryptographie les plus sûrs grâce aux attaques du cache. Au cas où nous ne serions pas parvenus à nos fins grâce à ce premier TP, un second fut l'occasion d'explorer les possibilités offertes par les injections de fautes, pour finalement s'infiltrer dans un système sans même disposer de la clé. Un troisième et dernier TP nous a introduit à l'audit matériel, en nous faisant exploiter les failles matérielles et logicielles présentent sur les plate-formes proposées.

Bien sûr, aucune école d'été ne mériterait ce nom sans les traditionnelles activités sociales. Sur ce point aussi, nous avons été largement servis : dès le premier jour, une visite de Rennes était proposée à ceux qui ne connaissait pas la ville, suivi d'un cocktail à l'hôtel de ville. Un « Capture The Flag » (série de challenges de sécurité informatique) a été également mis en place pour ceux qui souhaitaient mesurer leurs talents de hacker. Nous avons enfin passé un après midi fort agréable sous le soleil de Saint-Malo, avec pour les plus téméraires d'entre nous une excursion en catamaran sur les côtes bretonnes. Cette journée s'est terminée en beauté avec un repas de Gala à l'Escu de Runfao.

Pour ceux qui n'ont pas eu la chance d'assister à l'événement, certaines vidéos des présentations sont disponibles sur le site d'INRIA : `https://videos-rennes.inria.fr`. Un grand merci aux organisateurs, qui nous ont offert une semaine captivante, très riche en contenu, et qui plus est totalement gratuite.

Article rédigé par Matthieu Mastio, PostDoc, CNRS, IRISA, Contact : matthieu.mastio@irisa.fr

REDOCS 2019

La quatrième édition des Rencontres Entreprises DOCtorants en Sécurité informatique s'est déroulée du du 21 Octobre 2019 au 25 Octobre 2019 (`https://gdr-securite.irisa.fr/actualite/redocs-2019/`). Lors de cette édition trois entreprises (EDF, SystemX et Thales) ont proposé des sujets. Les trois équipes de cinq doctorants ont toutes réussi à proposer des solutions originales aux problèmes des industriels.

Proof of work REDOCS'19.

L'appel à participations des industriels pour l'édition 2020 de REDOCS est lancé. Les partenaires industriels qui souhaitent participer à cette cinquième édition peuvent dès à présent contacter `pascal.lafourcade@uca.fr`

Demandez les autocollants du GdR !

Ils ont été imprimés cet été, ils sont tous beaux, ils sont tous chauds : les autocollants, présents à REDOCS, seront aussi présents dans les prochaines manifestations du GdR, n'hésitez pas à tout faire pour vous procurer le vôtre, y compris en perçant les secrets du logo (voir Gazette numéro 2).

Avec l'autocollant REDOCS, le combo idéal !

Le coin prospectif

Pierrick Gaudry

La Gazette interroge Pierrick Gaudry, Directeur de Recherche CNRS au sein du LORIA. Son cœur de métier est la théorie algorithmique des nombres appliquée à la cryptographie. Depuis une demi-douzaine d'années, Pierrick s'intéresse également au vote électronique et il participe au développement de Belenios, un système de vote en ligne avec des garanties de vérifiabilité. Pierrick a récemment fait parler de ses travaux sur la mise à mal du système de vote électronique russe. Nous le questionnons sur ce point précis.

Bonjour Pierrick, comment t'es-tu rendu compte que le système de vote électronique russe possédait des faiblesses potentielles ?

La ville de Moscou a décidé de faire cette expérience de vote électronique pour ses élections de septembre, autorisant ainsi le vote par internet en parallèle du vote à l'urne classique dans 3 des 45 districts de cette élection. Dans ce cadre, un test public a été organisé, et une partie du code source a été diffusé. Lorsque j'ai appris l'existence de ce test, via des collègues académiques en Estonie, j'ai cherché dans le code la partie concernant le système de chiffrement, car je sais d'expérience que l'on y trouve parfois des erreurs. Quand j'y ai vu une variante inconnue du système ElGamal, je me suis dit que ça partait mal, car souvent les adaptations « maison » sont des mauvaises idées.

Peux-tu nous en dire plus sur l'attaque que tu as mise en œuvre ? À quelles difficultés as-tu dû faire face ?

L'algorithme de chiffrement s'est révélé être une sorte de triple-ElGamal, que j'imagine inspiré de triple-DES. Malheureusement, avec du chiffrement asymétrique, cela n'apporte essentiellement aucune sécurité supplémentaire par rapport à la taille de clef utilisée pour chacun des 3 chiffrements ElGamal imbriqués, contrairement au triple-DES qui permet d'émuler un système qui aurait une clef deux fois plus grande que pour un DES isolé.

In fine, casser ce système de chiffrement revenait à résoudre un problème de logarithme discret dans un corps fini de 256 bits. Une telle taille a été cassée pour la première fois dans les années 90, et aujourd'hui, en utilisant un outil spécialisé comme le logiciel CADO-NFS que nous développons au LORIA, cela ne prend que quelques minutes sur une machine de bureau. Notons toutefois que des logiciels standards (GP/Pari, Magma, Sage), prennent au moins une journée et parfois trop de RAM pour tourner sur une machine classique.

Mais la difficulté majeure n'était certainement pas le calcul de ces logarithmes discrets. Le problème principal était l'absence de documentation et encore moins de spécification complète du protocole. Comprendre le système de vote dans son ensemble uniquement à partir d'un code source est très difficile, voire impossible. Le cœur cryptographique était relativement simple à isoler dans le code, mais analyser l'impact de la faiblesse du chiffrement sur la sécurité du protocole global était loin d'être évident ; au début j'avais plus de questions que de réponses. Les interactions avec les organisateurs du test ont aussi été déroutantes. J'ai obtenu certaines informations complémentaires de leur part, mais ni documentation ni spécification permettant de faire une analyse satisfaisante du système.

Pierrick Gaudry.

« Nous avons forcé les concepteurs à mettre une porte blindée là où il y avait une porte grande ouverte, mais la maison tout autour reste en carton ! »

Que s'est-il passé depuis, est-ce que des correctifs ont été appliqués ?

J'avais rendu public un script permettant de refaire l'attaque de manière presque complètement automatique et un journaliste du journal russophone Meduza l'a effectivement fait tourner, si bien qu'il était difficile d'ignorer le problème. Le système de chiffrement a donc été modifié pour devenir un ElGamal classique avec une clef de 1024 bits, ce qui est encore petit, mais n'est attaquable qu'avec d'immenses ressources de calcul. En parallèle, ils ont également tenté de corriger une autre faiblesse que j'avais mentionnée. Toutefois, sur ce dernier point, leur correction n'était pas parfaite, comme révélé ensuite par un chercheur d'Harvard, Alexander Golovnev. Après une phase de déni de la part des concepteurs de Moscou, ils ont fini par corriger également cette deuxième vulnérabilité, juste avant l'élection proprement dite.

Néanmoins, l'impression que cela me laisse est mitigée. En effet, d'après ce que j'ai pu comprendre malgré l'absence de documentation, le reste du protocole de vote est globalement mauvais. Nous avons forcé les concepteurs à mettre une porte blindée là où il y avait une porte grande ouverte, mais la maison tout autour reste en carton !

Concevoir un protocole de vote est difficile, et les nombreuses propriétés que l'on souhaite sont en apparence contradictoires : on veut le secret du vote, mais en même temps de la transparence. Et dans un contexte très tendu comme les élections à Moscou il est également crucial de se prémunir des risques de coercition. Aucune de ces propriétés n'étaient réellement garanties, même avec un système de chiffrement fort.

Selon toi, quelles spécifications doit-on mettre en place pour rendre les systèmes de votes électroniques sûrs ?

Selon les contextes, les besoins peuvent être très différents et il n'y a pas de réponse universelle à ce qu'est un bon système de vote électronique. En effet, le système parfait n'existe pas encore, et il faut donc faire certains compromis en s'adaptant aux contraintes techniques, sociales et culturelles, tout en s'assurant toujours que l'on ne dégrade pas la sécurité par rapport au système que l'on remplace.

« Je considère que la Suisse a une bonne approche sur la question du vote électronique. »

Je considère que la Suisse a une bonne approche sur la question du vote électronique. Le législateur formule des exigences de sécurité, dépendant éventuellement des enjeux et de la proportion du corps électoral qui va utiliser la voie électronique. Ensuite les systèmes proposés doivent répondre à ces critères et notamment avoir des preuves de sécurité (comme dans nos articles académiques) en étant très clair sur les hypothèses de confiance. Et cela se termine par des tests publics où le code source est diffusé, ainsi que toute la documentation. La Suisse a par ailleurs montré récemment qu'en cas de doute sur la sécurité, elle n'hésitait pas à ne pas valider l'utilisation d'un produit, quitte à ce que pendant un certain temps le vote électronique ne soit plus disponible comme une option offerte aux électeurs.

En France, nous sommes loin de cette situation. Les recommandations de la CNIL ont le mérite d'exister, et leur mise à jour récente va dans le bon sens en demandant plus de garanties de vérifiabilité pour les élections à

fort enjeu. La nouvelle version lève aussi certaines restrictions obsolètes qui empêchaient d'utiliser des systèmes modernes. Mais une transparence des processus similaire à ce qui se fait en Suisse ne semble malheureusement pas encore à l'ordre du jour, y compris pour des élections à fort enjeu comme le vote des français de l'étranger aux législatives.

Quelle est/sera ta prochaine cible ?

Un système de vote appelé ElectionGuard a été rendu public par Microsoft ces dernières semaines aux États-Unis. Le contexte est différent du vote par internet, car il s'agit d'élections avec des machines à voter, dans des bureaux de vote. Le but des concepteurs est de fournir un SDK sous licence libre que les vendeurs pourront ensuite s'approprier, dans le but de les inciter à introduire plus de vérifiabilité dans leurs systèmes. À Nancy nous avons commencé à regarder la spécification et le code de référence. Il s'agit encore de beta-versions, mais nous avons déjà un certain nombre de commentaires qui devraient nous aider à améliorer un produit qui sera potentiellement déployé à grande échelle.

Tes recherches œuvrent donc pour la démocratie numérique, merci Pierrick et bonnes vérifications !

Article rédigé par Pierrick Gaudry (CNRS, LORIA), Annelie Heuser et Patrick Bas, Contact : pierrick.gaudry@loria.fr

Un artiste sommeille en vous ?

Vous êtes dessinateur ? poète ? verbicruciste ? poseur d'énigmes ? ... la gazette peut vous faire une petite place pour vous exprimer si cela touche de prêt ou de loin à la sécurité. N'hésitez pas à contacter des membres l'équipe éditoriale pour soumettre vos idées.

Jobs

(Repris en partie du forum du GDR)

CDD Ingénieur de recherche (IR), Railenium (Villeneuve d'Ascq ou Valenciennes)

Titre : Ingénieur Analyse des risques cybersécurité
Contact : Christophe Gransart, christophe.gransart@ifsttar.fr, recrutement@railenium.eu

Enseignant second degré, Université Clermont Auvergne (Clermont-Ferrand)

Discipline : Mathématiques option Probabilités et Statistiques. ***Contact : Béatrice COLLAY, beatrice.collay@uca.fr, et Olivier GUINALDO, Olivier.guinaldo@uca.fr, et Michel MISSON, michel.misson@uca.fr***

Offre de thèse, Eurecom (Sophia-Antipolis)

Titre : Security of IoT devices in 5G networks through fingerprinting and side-channel analysis
Contact : Aurélien Francillon, aurelien.francillon@eurecom.fr, et Clémentine Maurice clementine.maurice@irisa.fr

Offre de stage, IRISA (Rennes)

Titre : Simulating Transient Execution Attacks with gem5
Contact : Clémentine Maurice clementine.maurice@irisa.fr, Annelie Heuser, annelie.heuser@irisa.fr

Offre de stage, IRISA (Rennes)

Sujet : malware analysis, side-channel analysis
Contact : Olivier Zendra, olivier.zendra@inria.fr, Annelie Heuser, annelie.heuser@irisa.fr